UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple iCloud Accounts assigned to kingmadellc.com, DSID: 17353251428; and zakayanthonyking@icloud.com, DSID: 8320609572

Case No. 23- 246M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of Delaware , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 286	Conspiracy to File False Claims
18 U.S.C. § 287	False Claims
18 U.S.C. § 7206(1)	False Return

The application is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Antonino Lo Piccolo
Applicant's signature

IRS SO Antonino Lo Piccolo
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: 05/31/2023

Christopher J. Burke
Judge's signature

City and state: Wilmington, Delaware

Christopher J. Burke, US Magistrate Judge
Printed name and title

Print Save As... Attach Reset

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Antonino Lo Piccolo, Special Agent, United States Department of Treasury, Internal Revenue Service Criminal Investigation ("IRS-CI"), being duly sworn, state:

I. INTRODUCTION

1. I am employed as a Special Agent ("S/A") with IRS-CI and have been since August 19, 2004. I received a Bachelor of Science Degree in Accounting from the Pennsylvania State University in 1999. I am currently assigned to the Philadelphia Field Office, Newark, Delaware, post-of-duty. In connection with my official duties as an IRS-CI S/A, I investigate criminal violations of federal tax law, including willful filing of a False Return (26 U.S.C. § 7206(1)), and False, fictitious, or fraudulent claims (18 U.S.C. § 287)

2. I graduated from the Federal Law Enforcement Training Center ("FLETC") on February 11, 2005. There I received instruction on investigative techniques and searches and seizures. I have been trained in the execution of financial search warrants resulting in the seizure of financial documents, and tax-related documents. As a federal agent, I am authorized to investigate violation of laws of the United States, including the crimes outlined herein, and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a search warrant regarding information associated with certain accounts, that is, the "**SUBJECT ACCOUNTS**," that are stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California.

    a. SUBJECT ACCOUNTS: The iCloud accounts assigned Apple Credential IDs:

    kingmadellc@icloud.com and **DSID: 17353251428**;

    zakayanthonyking@icloud.com and **DSID: 8320609572;**

4. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items.

5. The United States is investigating ANTHONY KING (hereinafter "KING") for possible violations of, Title 18, United States Code (U.S.C.) Sections, 286 and 287 (Conspiracy to File False Claims and False Claims, and Title 18, U.S.C. Section 7206(1) (False Return) (collectively, the "Subject Offenses"). The facts set forth in this Affidavit are based on my personal observations, my training and experience, information obtained from other special agents and analysts, subpoenaed records, and IRS records. Because I submit this Affidavit for the limited purpose of showing probable cause, I have not included in this Affidavit each and every fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue a search warrant for the SUBJECT ACCOUNTS.

THE RELEVANT FACTS

SUMMARY

6. As set forth below, there is probable cause that KING electronically submitted 28 Form 1040 U.S. Individual Income Tax Returns ("Form 1040") for the 2021 or 2022 tax years on behalf of others and himself, seeking payment of $830,737 in tax refunds based on false W-2 federal income tax withholding amounts or false COVID-19 related sick leave tax credits claimed on the returns. As a result of the filings, the Internal Revenue Service ("IRS") issued $369,724 in fraudulently obtained refunds.

7. The Family First Coronavirus Response Act (FFCRA), passed in March 2020, allows eligible self-employed individuals who, due to COVID-19 are unable to work or telework for reasons relating to their own health or to care for a family member to claim refundable tax credits to offset their federal income tax. Eligible self-employed individuals determine their qualified sick and family leave equivalent tax credits ("SLC") using IRS Form 7202, Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals ("Form 7202"). The amount of the credit is determined by dividing the total amount of self-employment earnings during either the current or prior year by 260 days and then multiplying that figure by the number of days missed due to a COVID-19 illness or quarantine between January 1, 2021 and March 31, 2021 and April 1, 2021 and September 1, 2021. The two figures are then added together for the total SLC available for 2021. The SLC is a refundable tax credit meaning the SLC can result in the taxpayer receiving a refund exceeding the total amount of tax withholdings and estimated tax payments made by the taxpayer during the year. In other words, a refundable tax credit creates the possibility of a negative federal tax liability.

8. Form W-2 is an IRS tax form used by employers to report wages paid to employees and the taxes withheld from them to the IRS. Employers must complete a Form W-2 for each employee to whom they pay a salary, wage, or other compensation as part of the employment relationship. The Employer provides a copy of the Form W-2 to its employee to include when the employee files his or her income tax return and a copy to

the IRS. An Employer Identification Number ("EIN"), also known as the Federal Employer Identification Number or the Federal Tax Identification Number, is a unique nine-digit number assigned by the IRS to business entities for the purposes of identification. An employer includes its EIN on Forms W-2 issued to the IRS and to its employees so the IRS can match the information contained on the W-2's

THE INVESTIGATION

9. In or around October 2022, a representative of Republic Bank contacted an IRS-Criminal Investigation Special Agent ("IRS-CI S/A"), regarding an accountholder who received a suspiciously large tax refund. Republic Bank advised the IRS-CI S/A that prior to receipt of the tax refund the account had been dormant over a year and that the accountholder conducted two large cash withdrawals after the deposit of the tax refund.

10. The IRS-CI S/A obtained and reviewed the Republic Bank accountholder's 2021 Form 1040 and determined the accountholder received a tax refund in the amount of $31,422, primarily as the result of claiming a SLC in the amount of $30,050. Your affiant reviewed the SLC information presented on the Form 7202 and found the accountholder claimed he earned $130,262 in self-employment earnings in the prior year and lost 100 days of self-employment earnings in 2021 due to COVID-19. IRS-CI obtained and reviewed the Republic Bank accountholder's 2020 Form 1040 and found that the accountholder only reported $3,010 in self-employment earnings for 2020, therefore the Form 7202 SLC was calculated and paid based on false information.

11. IRS-CI determined the Republic Bank accountholder's 2021 Form 1040 was electronically submitted to the IRS from an internet connection assigned IP address 68.83.231.101 ("the Comcast IP address"). This IP address is registered to Comcast. Based on IRS records, 19 additional tax returns for the 2021 tax year were filed between June 23, 2022 and October 28, 2022 from this same IP address. Records obtained from Comcast show this IP address was assigned to internet service provided to KING at his Bear, Delaware residence from at least as far back as August 9, 2022. KING's own Form 1040 was submitted to the IRS on June 23, 2022, from the Comcast IP address.

12. A SLC is claimed on each 2021 tax return filed from the Comcast IP address. Each credit claimed was calculated based on the loss of 100 days self-employment wages due to COVID-19 and a prior year self-employment earnings figure. IRS-CI compared the prior year self-employment earning figures on Form 7202 to amounts reported on the individuals' 2020 tax return. IRS-CI found that eight of the individuals had not filed a 2020 tax return and another eight individuals filed a 2020 tax return that did not report any self-employment earnings. The remaining two individuals reported 2020 self-employment earnings of $5,746 and $17,736 respectively, which are substantially less than the amounts, greater than $130,000, that are claimed on the individuals' Forms 7202.

13. IRS-CI noted other commonalities between the 2021 Forms 1040 reviewed. 18 of the 19 tax returns listed Barber, Hairdresser, or Hairstylist as the individual's occupation. 17 of the 19 tax returns list on Form 7202 a prior year self-employment earnings amount between $130,000 and $130,262, with six listing exactly $130,262 in prior year self-employment earnings. All 19 returns were submitted to the IRS using Intuit tax return preparation software.

14. The SLC has been discontinued for the 2022 tax year and is not available for taxpayers to claim when filing their federal income tax returns for the 2022 tax year during the current 2023 filing season. The 2023 filing season began on January 23, 2023. Beginning on January 25, 2023 through February 7, 2023, the IRS received nine 2022 Forms 1040 from the Comcast IP address assigned to internet service provided to KING. All nine returns were filed using Intuit tax return preparation software. The nine returns include KING's own 2022 Form 1040 and eight others reporting W-2 wages purportedly earned from employment with DL NEU & Associates (hereinafter "DL"). DL's address is listed as 7885 Byron Center Ave Byron Center, MI 49315 on the W-2s.

15. DL's Office Manager told an IRS-CI S/A that DL moved from the address shown on the W-2s approximately seven years ago and that DL changed names to DLN Integrated Systems, Inc. in 2019. When asked to verify employment of the eight individuals whose returns included a W-2 purportedly from DL, the Office Manager advised the IRS-CI S/A that the individuals were never employed by DL or DLN Integrated Systems, Inc.

16. On March 16, 2023, at approximately 8:30AM, IRS-CI S/As conducted a search warrant (23-97M authorized on March 14, 2023 by the Honorable Sherry R. Fallon) at KING's residence. The IRS-CI S/As encountered KING, who confirmed he lived at the location with his children. From a nightstand in the master bedroom, IRS-CI seized handwritten notes containing names, social security numbers, dates of births, addresses, bank routing and account numbers, and dollar amounts matching the returns filed from the Comcast IP address. IRS-CI also seized a printed copy of an electronically filed tax return, filed in the name of an individual other than KING, on which a fraudulent SLC was claimed.

17. Several pages of the seized handwritten notes were examined for latent fingerprints by IRS-CI's Center for Science and Design. The technique applied during the examination developed seven latent prints suitable for comparison to KING's fingerprints obtained during a prior arrest. All seven latent brings from the handwritten notes were found to match KING's fingerprints.

18. As of May 2, 2023, IRS-CI has spoken with five individuals for whom a 2021 return and/or a 2022 tax return was filed from the Comcast IP address, and whose personal information was listed in handwritten notes located at KING's residence. Three of the five individuals confirmed they provided KING their personal information via text messages for the purpose of filing a 2021 tax return. The others confirmed they gave

KING their information to complete a tax return but could not recall if the information was sent by text. Each gave (267) 984-0403 as KING's cell phone number. This same phone number is listed on KING's 2021 and 2022 tax returns and on KING's leasing application submitted for his current residence. Each of the five individuals denied telling KING they had 2020 self-employment earnings in the amounts listed on their returns to generate the SLC claimed and received. Specifically, one person that IRS-CI spoke with is 74 years old and has been retired since at least the year 2000.

19. IRS-CI obtained and reviewed records produced by T-Mobile (267) 984-0403, including call logs. A total of 21 different individuals had either a 2021 or 2022 tax return filed that is a subject of this investigation. A different cell phone number is listed on each tax return as belonging to the individual in whose name the return was filed. Of those 21 individuals/cell phone numbers, 16 were found to have exchanged, on or about the date their return was filed with the IRS, either a text message, phone call or both with phone number (267) 984-0403.

20. Between July 7, 2022 and September 8, 2022, the IRS released refunds totaling $369,724 as a result of tax returns electronically filed in this scheme. The five individuals interviewed by IRS-CI to date each paid KING a fee between $7,500 and $12,000 for the filing of their returns. They paid KING his fee using a combination of cash, cashier's checks, and peer-to-peer ("P2P") electronic service payments Cash App and Apple Cash. Between July 7, 2022 and September 8, 2022, KING received into a Citizens Bank account, held in his name and on which he is the only signer, approximately $19,500 in Apple Cash and $6,850 in Cash App transfers.

21. Apple Cash, which includes the ability to send and receive money person to person with messages and the Apple Cash Card, is a service provided by Green Dot Bank. Your affiant reviewed records obtained from Green Dot for the Apple Cash account linked to zakyanthonyking@icloud.com and phone number (267) 984-0403. The account was opened under the name "Manny Young king" using KING's social security number and date of birth. The data indicates from July 8 to August 24, 2022, KING received payments from at least four individuals who had a fraudulent return filed. For four of the individuals, a transfer was made the same or the day following the receipt of a tax refund. For example, on August 24, 2022, the IRS issued L.W. a $31,423 refund. The Green Dot records shown L.W. transferred $8,000 to KING's Apple Cash account on the same day.

22. P2P transfer services commonly utilize mobile devices and request or receive money into accounts based on e-mail addresses. Through review of bank records, loan applications, and tax records, IRS-CI has determined KING uses email addresses Kingmadellc@icloud.com and zakyanthonyking@icloud.com. On March 16, 2023, IRS-CI submitted a request to Apple, Inc. to preserve all records associated with the two email addresses for a period of 90-days.

23. During the search warrant conducted on March 16, 2023, IRS-CI seized a MacBook Air 9,1 laptop from KING's master bedroom. The screensaver on the MacBook is a picture of KING. IRS-CI is unable to examine the contents of the computer as the device is encrypted. KING declined to provide his passcode to enable IRS-CI access to the computer's contents. KING was also found to be in possession of a locked Apple iPhone. KING also declined to provide IRS-CI with the passcode to his phone.

24. On April 10, 2023, Apple, Inc., pursuant to an Order issued under 18 U.S.C. § 2703(d) by the Honorable Christopher J. Burke, produced records and subscriber information for the accounts associated with email addresses Kingmadellc@icloud.com and zakyanthonyking@icloud.com.

25. Apple's response to the Order showed that Subject Account Kingmadellc@icloud.com, that is, KING's account, was created on or about July 23, 2020, under the name ANTHONY KING and phone number (267) 984-0403. Apple also produced records and information about the features activated for Kingmadellc@icloud.com. The account has activated iCloud backup, which pertains to backups of iOS devices associated with the account. It also has activated backups of specific apps, including Bookmarks, Calendars, iCloud Photos, Contacts, iCloud Drive, Mail, Mail Header, Notes, and Sign In with Apple. Data provided in Apple's response indicates the Advanced Data Protection software is not currently being utilized and the most current device associated with the account is a MacBook Air 9,1.

26. Apple's response to the Order also showed that Subject Account zakyanthonyking@icloud.com, that is, KING's account, was created on or about May 5, 2015, under the name ANTHONY KING and phone number (267) 984-0403. Apple also produced records and information about the features activated for zakyanthonyking@icloud.com. The account has activated iCloud backup, which pertains to backups of iOS devices associated with the account. It also has activated backups of specific apps, including Bookmarks, Calendars, iCloud Photos, Contacts, iCloud Drive, Mail, Mail Header, Notes, Sign In with Apple, and Safari Browsing History. Data provided in Apple's response indicates the Advanced Data Protection software is not currently being utilized and an iPhone was backed-up as recently as April 3, 2023 – the date the 2703(d) was issued.

27. Your affiant reviewed email header information provided by Apple Inc. for accounts kingmadellc@icloud.com and zakyanthonyking@icloud.com. The header information reflects the dates, the sending and receiving addresses of email communications. Zakyanthonyking@icloud.com is the email address listed on KING's 2021 and 2022 Forms 1040. The header information shows the receipt of emails from an Intuit email account on June 23, 2022 and February 7, 2023, the respective filing dates of KING's 2021 and 2022 Forms 1040.

28. Your affiant's review of the email header information revealed both kingmadellc@icloud.com and zakyanthonyking@icloud.com were used to send emails to addresses associated with individuals who had a fraudulent return filed. For example, a 2021 Form 1040 was filed for Anqelique W. on July 8, 2022. The corresponding $31,425 refund was paid August 31, 2022. In between two emails were sent from kingmadellc@icloud.com to email address Wangelique527@gmail.com. This email appears on tax returns filed for Anqelique W. in previous years.

Background Concerning Apple[1]

29. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

30. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

    a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

    b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

    c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet- connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law- enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

e. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

f. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

31. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Apple uses the DSID, or Directory Services Identifier, as an internal identifier for accounts. Users can submit an Apple- provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

32. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the

account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

33. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

34. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

35. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud

Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

36. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

37. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

38. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

39. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

40. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

Conclusion

41. IRS-CI is investigating the electronic filing of tax returns submitted from an IP connection assigned to KING's residence. KING has communicated with individuals by text message using a cellular telephone in connection with the filing of false federal income tax returns. In addition, individuals known to have received fraudulently claimed tax refunds paid KING a fee for his involvement in filing their return using peer-to-peer transfers and received emails from accounts belonging to KING. The facts set forth in

the previous section show that there is probable cause for a search warrant authorizing the examination of the SUBJECT ACCOUNTS outlined in Attachment A and to seek the items described in Attachment B.

Antonino Lo Piccolo

Special Agent Antonino Lo Piccolo
IRS- Criminal Investigation

Sworn to and subscribed before me
on this 31st day of May, 2023

Christopher J. Burke

Christopher J. Burke
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with:

SUBJECT ACCOUNTS: The iCloud accounts assigned Apple Credential IDs:

kingmadellc@icloud.com and **DSID: 17353251428**;

zakayanthonyking@icloud.com and **DSID: 8320609572**

ATTACHMENT B
Particular Things to be Seized

I. **Information to be disclosed by Apple Inc. ("Apple")**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account from January 1, 2021 to Present, including stored or preserved copies of instant messages (including iMessages, SMS messages, WhatsApp, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact

and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, WhatsApp, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 26, United States Code, Section 7206(1) False Return and United States Code, Section 287, False, fictitious, or fraudulent claims, and United States Code, Section 286, Conspiracy to file false claims for the period from January 1, 2021 through the present day, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Books, notebooks, records, documents, bills, receipts, data, images, videos, or information relating to such offenses, including any records or documents or other evidence regarding:

b. The filing of federal or state tax returns,

c. Communication, notes, documents, and other records containing identity

information (including names, social security numbers, and dates of birth),

d. Financial or other transactions involving fraudulently obtained funds, including any information regarding currency, checks, or other financial instruments relating to illicit proceeds, including the use or spending of such proceeds,

e. Financial records, bank records, checkbooks, payroll information, ledgers, or other financial information pertaining to ANTHONY KING, KINGMADE LLC, and individuals for whom a tax return was filed from the Comcast IP,

f. Any federal or state income tax returns, tax return information, supporting information and documentation, including all drafts and final productions, along with all Forms W-2, Forms 1099, Wage and Tax Statements, IRS publications, instructions, and similar forms, filed or not filed, and supporting work papers used in preparation of tax returns.

g. Records of internet activity, including firewalls logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses relating to the unlawful conduct described above,

h. Evidence of who used, owned, or controlled the digital device or other electronic storage media linked to the SUBJECT ACCOUNTS at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat", instant messaging logs, photographs, and correspondence,

i. Communications, including but not limited to iMessages, SMS, and MMS, WhatsApp stored voice mail, voice memo, or other audio messages, recordings of incoming calls, calendar information related to the to the unlawful conduct described above.

j. Photographs of ANTHONY KING and possible co-conspirators, their property, their assets, and currency which could constitute evidence of the unlawful activities described.

k. Records and information, including GPS, that reflects other known associates, and possible conspirators in furtherance of the conduct described above.